Qualys

NEW QUALYS CEO TACKLES CYBERSECURITY ASSET MANAGEMENT

Sumedh Thakar Outlines Vision to Reduce Complexity and Enhance New Security Landscape

ISMG
INFORMATION SECURITY
MEDIA GROUP

SUMEDH THAKAR

As CEO, Thakar leads the company's vision, strategic direction and implementation. He joined Qualys in 2003 in engineering and grew within the company, taking various leadership roles focused on helping Qualys deliver on its platform vision. Since 2014, he served as chief product officer at Qualys, where he oversaw engineering, development, product management, cloud operations, DevOps and customer support. He is a driving force behind the rollout of the game-changing VMDR – vulnerability management, detection and response – which continually detects and prevents risk to their systems, and multi-vector EDR, which focuses on protecting endpoints, as well as container security, compliance and web application security solutions. He was also instrumental in the buildup of multiple Qualys sites, resulting in a global 24/7 "follow the sun" product team.

Longtime Qualys leader Sumedh Thakar recently was named CEO of the company. Now he's laying the groundwork for a long-term vision that includes helping customers adjust to the new enterprise security landscape and embrace cybersecurity asset management.

In a video interview with Information Security Media Group as part of its RSA Conference 2021 coverage, Thakar discusses

- His leadership vision as CEO;
- The shifting security landscape;
- The role of cybersecurity asset management.

THAKAR'S JOURNEY AT QUALYS

FIELD: Tell us about your journey and how it shapes how you now will lead Qualys.

THAKAR: I started at Qualys over 18 years ago as a software engineer and through that, I experienced both the IT and the security side of the house as we grew the company. We were one of the first companies to

have what is now called a cloud-based platform, but a SaaS platform, and I learned a lot about the challenges that the IT teams face when it comes to security. Qualys' culture is to learn from our customers to understand their problems and find solutions for them. This customer point of view has shaped the way I look at and bring products and solutions to market.

THAKAR'S LONG-TERM VISION

FIELD: As you look forward, what's your long-term vision for Qualys?

THAKAR: The vision is to work together to build a platform that simplifies the security deployment and the number of solutions that you need to make it work and to get the visibility that you need. Cybersecurity today is too complex. A lot of CISOs will tell you that they have anywhere from 30 to 80 different individual solutions. I can't think of any other technology field in which you need so many solutions to make something work. The vision for us, and what we have been executing in the last few years, is bringing multiple aspects of security onto a single, simplified platform.

Our long-term vision is to continue to put innovation onto the platform so that we can continue to make it less complex. Today there are too many silos. There's a solution that looks at inventory, another one that looks at prevention and another one that looks at detection. And the customers have to glue all of that together. Security needs to be more like AWS or GCP. These cloud platforms are popular because the customer gets everything they need, such as processing power, memory and storage, all in one place. They don't have to go to multiple vendors to get CPU's from one vendor and storage from another.

SECURITY SOLUTIONS CUSTOMERS NEED

FIELD: What solutions do customers need to navigate a rapidly changing security landscape that is so different today than it was even a year ago?

THAKAR: If you look at the basics of security, you need three things. First, you need to know what assets you have across your cloud and on-premises environment and the particulars of that asset. For example, is the asset a lab machine? Does it run a production database? Second, you need to continuously mitigate risk with preventive controls - assessing images for vulnerabilities and identifying missing patches and misconfigurations before and after they go into production. Third, you need to monitor the environment for the latest threats and correlate telemetry for a quick and apt response.

Security is not our customers' main business. They have different businesses that they're running. They want their data and their customers' data to be secure. And that requires a lot more automation and a lot more ability to get security out of the way, in a positive way, where it's taken care of. Detecting problems and taking action quickly with automation is the future of security, where it becomes less intrusive than what it is now.

EFFECTS OF THE PANDEMIC ON SECURITY

FIELD: How has the pandemic experience affected the enterprise cybersecurity trajectory? What changes do you see in customer needs today versus a year ago?

THAKAR: As the pandemic pushed employees to work remotely, SaaS application use exploded because it provided access to remote employees. This change also caused organizations to rethink their perimeter. They turned to cloud-based security solutions that could scale and protect those remote endpoints and SaaS application data without the need for a VPN.

Earlier, you had maybe 3% or 5% of your workforce outside your network, and now we have a customer who has 250,000 employees globally, each with their individual laptop, sitting in an apartment somewhere in the world on a home network, broadband. How do you protect those devices? How do you even know what you have and where these devices are?

A PLATFORM-DRIVEN APPROACH

FIELD: There are more choices than ever, and it's been boom times for cybersecurity companies and startups. In fact, there are so many cybersecurity vendors and solutions these days, it adds to the degree of complexity. How does this affect the customer who is trying to make sense of all of this in the marketplace?

THAKAR: People are trying to find new and different ways to simplify security, but they are looking at it as solving one specific problem at a time. So every little feature ends up becoming a product deployment, which then ends up becoming complex and hard to deploy and manage, and needs more people to figure out how one thing relates to another. The best of breed approach worked when you had five or 10 solutions. But now that you have about 50 solutions, which don't talk to each other and what's more, you need yet another tool to aggregate the data. We need more of a platform-driven approach. Every vendor is trying to say that they have a platform. That's where the opportunity is for cybersecurity innovators. It's not just about whether you have the latest feature; It's also about what you are doing to simplify your customers' deployments, how you provide intelligence on their true risk, and what insights you give to help them protect their environment. No CISO says, "I want more security solutions."

“A solution that is focused on inventory for cybersecurity will help security teams identify all their assets in real time so that they can build a solid program around them.”

CYBERSECURITY ASSET MANAGEMENT

FIELD: Tell me about cybersecurity asset management.

THAKAR: Asset management has been a big challenge for everybody. It is the cornerstone. You start your security program by knowing what you have. The security teams rely on the IT teams to figure out what the assets are, but IT teams look at assets in a different way than security teams do. IT teams look at the life cycle: When was it purchased? Is it still supported? Is the warranty is still active? They ignore the data collection capability that a cybersecurity team needs. Security teams want to know: Is the software current or end-of-life? What unauthorized software is installed? Which assets are high criticality? Typically IT teams don’t care about this kind of context, but the security team does.

Customers need to discover what they have. It’s a difficult job, because you need a combination of agent-based and agentless sensors. Next, customers need to know what’s on those assets and have basic policies to ensure that those assets are not running things that they should not be running. Traditional vulnerability management solutions don’t necessarily help because the software may not have any vulnerabilities. We’ve created a way for our customers to focus on asset inventory from a cybersecurity aspect.

CYBERSECURITY-FOCUSED ASSET INVENTORY

FIELD: One might think of asset inventory is an IT issue. Why is it so critically important for security teams?

THAKAR: It's the starting point of any cybersecurity program. Configuration management databases can be referenced by security teams but aren't themselves accurate and complete enough to solve their use cases. And the same is true for typical IT Inventory repositories. Cybersecurity teams need more specific data collection and policies than IT teams. A solution that is focused on inventory for cybersecurity will help them identify all their assets in real time so that they can build a solid program around them and be able to collect additional pieces of information that typically are not collected by the IT solutions.

THE EFFICIENCY OF AUTOMATION

FIELD: You emphasized taking action by using the same solutions. Is this something that your customers demanded?

THAKAR: Customers want to focus on their main business and take care of IT and security issues quickly. We're seeing automation in IT and more and more in cloud. People are open to automation, without humans being involved, and that saves a lot of time. So we want to bring those concepts to security as well. We want to take action quickly. Today, because there are too many tools, there is a lack of confidence in the detection. And when you're not confident that the detection is accurate, you're not going to take a response action. But as we build solid solutions that bring more context and automation, the confidence level will rise.

If you have a policy in place that says, "I should not see a messaging software being installed on my web server," we can, with the same solution, the same agent, also based on a policy, uninstall that software instead of taking the time to create a ticket and have somebody look at it. If there is a clear violation, there will be a response action. The idea of taking action without human intervention was pioneered by EDR solutions. People don't want to work through volumes of PDF reports; more and more, they want to take response actions from within the apps themselves.

Qualys®

About Qualys.

The leading provider of information security and compliance cloud solutions.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® (Just for Credit Unions) GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY (Prevention. Response. Notification.) CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io